UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/483,358	01/14/2000	Ernst-Michael Hamann	GE-99-008	8276

7590 12/08/2004

James E Murray
69 South Gate Drive
Poughkeepsie, NY 12601

EXAMINER	
KIM, JUNG W	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 12/08/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/483,358	HAMANN ET AL.	
	Examiner	Art Unit	
	Jung W Kim	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 October 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-15 and 17-25* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-15 and 17-25* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *23 February 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on Octoer 25, 2004 has been entered.

2. Claims 1-15 and 17-25 have been examined. Applicant in the amendment filed on October 25, 2004 amended claims 1, 3, 4, 6, 10, 15, 19, 22 and 24, and canceled claim 16.

Response to Arguments

3. The following is a response to applicant's arguments and remarks on pages 19-24 of the amendment filed on October 25, 2004.

4. Applicant's arguments with respect to claims 1-5 and 17-25 have been considered but are moot in view of the new ground(s) of rejection.

5. In regards to applicants inquiry of the statutory basis that restricts patentability of an invention having subject matter that as a whole would have been obvious to one of

ordinary skill in the art at the time the invention was made (page 24, second paragraph), examiner points to 35 U.S.C. 103(a).

Claim Objections

6. Claims 1, 15 and 19 are objected to because of the following informalities: in claim 1, step a), the word "recitation" is misspelled; in claim 15, step c), the word "chipcard" is misspelled; in claim 19, preamble, the phrase "issuer to the certificate" should read "issuer of the certificate". Appropriate correction is required.

Claim Rejections - 35 USC § 112

7. Regarding claims 1, 4, 8, 10, 19 and 22, the phrases "(issuer of the certificate)" in claims 1, 8, 10 and 19, and "(group certificate)" in claims 4, 8 and 22, render the claims indefinite because it is unclear whether the limitation(s) in parenthesis are part of the claimed invention. See MPEP § 2173.05(d).

8. Regarding claims 5, 9 and 23, the phrase "type/version" in claims 5, 9 and 23 extends the scope of the expression so as to render the claims indefinite because it is unclear what "type/version" was intended to convey. See MPEP § 2173.05(b).

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 1-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over VeriSign 'Certification Practice Statement' version 1.2 (hereinafter VeriSign) in view of Stallings Cryptography and Network Security 2nd Edition (hereinafter Stallings), Sutter U.S. Patent No. 5,924,094 (hereinafter Sutter), Karlton 'Proposal to add attribute certificates to TLS 3.1' (hereinafter Karlton) and Silberschatz et al. Database System Concepts 3rd edition (hereinafter Silberschatz).

11. As per claim 1, VeriSign discloses a method of creating a certificate to certify a key, wherein the certificate comprises a defined number of data elements which at least contain information on the certification body, the user of the certificate and the key certified by the certificate (see VeriSign, sec. 2.4.9, fig. 3), comprising the following steps:

a. creation by the certification body of a basic certificate for the user containing a single recitation of a defined number of data elements therein which elements are identical or redundant for the several keys of the user in conjunction with the certification body (see VeriSign, sec. 4.2, class 1 type, 'Method of Communicating Application');

b. addition of an identifying characteristic to the basic certificate (see VeriSign, sec. 2.4.9, fig. 3, 'serial number').

2. Further, VeriSign does not expressly disclose signing an issued certificate. However, Stallings teaches digital signatures are a conventional methodology to enable

the receiver of the message to verify the origin of a given message. See Stallings, page 300, 1st 3 bullets. More specifically, Stallings discloses X.509 certificates are conventionally signed to verify a given certificate was generated by a trusted CA. See Stallings, pg. 342, fig. 11.3, especially signature data fields. It would be obvious to one of ordinary skill in the art at the time the invention was made for the CA to sign an issued certificate. Motivation to combine include, inter alia, enabling the certificate applicant to verify the CA issued a signed certificate. Ibid. Hence, the method covered by the teachings of VeriSign and Stallings further includes the following steps:

c. generation and addition of a digital signature to the basic certificate (see Stallings, Ibid.);

d. generation of a key pair: inherent in the inclusion of a public key data value in the certificate disclosed by VeriSign is the generation of a key pair - public and private keys (see VeriSign, Ibid.; see Stallings, pg. 342, fig. 11.3, subject's public-key info data field).

3. Furthermore, VeriSign does not disclose certifying a plurality of keys for a user in a single request. Sutter discloses a plurality of keys being certified as a single certificate. See Sutter, 49:35-39. It would be obvious to one of ordinary skill in the art at the time the invention was made to apply the teaching of Sutter to the invention covered by VeriSign. Motivation to combine include, inter alia, enabling the plurality of keys used for different purposes by the subscriber to be assigned as one certificate as taught by Sutter. Ibid.

4. Moreover, VeriSign does not disclose the creation of a certificate beyond the basic certificate. However, it is well established in the art the X.509 protocol does not meet many of the requirements that new and emerging secure network transactions require, specifically the need for a user to have multiple keys for different types of transactions. Examples of efforts to extend the scope of the certificate methodology disclosed by VeriSign to handle this requirement including the following: X.509 v3 protocol includes extensions to the basic certificate format (see Stallings, pg. 348, 'Key and Policy Information'); Sutter, above, incorporates a plurality of keys within one certificate; and, Karlton discloses an attribute certificate having similar syntax as an X.509 v3 certificate to further extend the use of an identity certificate. See Karlton, entire document. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to create a certificate methodology beyond the framework of the basic certificate, which merely associates one user to one key, wherein the one key has only one use. Motivation to combine include, inter alia, enabling a certificate methodology to handle the requirements of new and emerging secure network transactions as taught by Stallings, Sutter and Karlton. Ibid.

5. Additionally, VeriSign does not disclose a supplementary certificate as defined in the limitations of applicant's claim. However, certificates are in essence a model for storing user information, key values and the relationships between users and key values (see Stallings, pg. 342, fig. 11.3, 'X.509 attributes'; pg. 348, 'Key and Policy Information'; pg. 349, 'Certificate Subject and Issuer Attributes'; see Sutter, 49:35-39), as well as the relationships among users (see Stallings, pg. 345, fig. 11.4, 'X.509

hierarchy'; pg. 349, 'Certificate Subject and Issuer Attributes' and 'Certification Path Constraints'); and data models congruent with the role of a supplementary certificate in relation to the role of a basic certificate is known in the related art of database design. Silberschatz teaches an entity-relationship (E-R) model wherein a basic entity containing a single recitation of a defined number of data elements, which elements are identical or redundant for several auxiliary attributes of the basic entity, which auxiliary attributes are contained in supplementary entities. See Silberschatz, pgs. 7-8, sec. 1.3.1.1; pgs. 52-58, esp. figs. 2.20, 2.21, 2.22 and sec. 2.9.3.2; in the bank example, each customer record is a basic entity which corresponds to a basic certificate, and each borrower record is a supplemental entity which corresponds to a supplemental certificate wherein the loan-number is a auxiliary attribute which corresponds to the certified key. Moreover, the basic entity is used in conjunction with the supplemental entities, each supplemental entity containing one of the auxiliary attributes and the identifying characteristic of the basic entity, and each supplemental entity containing additional data fields not recited in the basic certificate; and the redundant information recited in the basic certificate is not recited in each supplemental entity. See Silberschatz, pg. 55, fig. 2.22. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to apply the teachings of Silberschatz to the method of VeriSign. Motivation to combine include, inter alia, enabling logical data modeling of certificate keys utilized in new and divergent types of digital transactions (users need a distinct signature verification key for each distinct type of digital transaction). See Silberschatz, pg. 7, last sentence; see Sutter, 49:35-39. Finally, as

taught by Stallings above, certificates are conventionally signed to authenticate the creator of the certificate, to attain user's confidence in the certified signatures on digital transactions. Hence, the method covered by the teachings of VeriSign, Stallings, Sutter and Karlton and Silberschatz further includes the following steps:

e. creation of a supplementary certificate for the basic certificate which does not recite the redundant data elements but does contain a key as set out in step d, the identifying characteristic as set out in step b and additional data fields not registered by the basic certificate (see Silberschatz, Sutter, Ibid.);

f. generation and addition of a digital signature to the supplementary certificate (see Stallings, Ibid.);

g. use of the basic certificate created in step a for other of the several keys in additional supplementary certificates that share with the supplementary certificate of step e the redundant information recited the basic certificate but like the supplementary certificate of step e do not recite the redundant data elements (see Silberschatz, Ibid).

The aforementioned cover the limitations of claim 1.

6. As per claim 2, VeriSign covers a method as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). In addition, the basic certificate comprises the following data elements: name of certification body, user id of certification body, name of user, user id of user, and identifying characteristic of the basic certificate. See

Stallings, page 342, Figure 11.3 (a). The aforementioned cover the limitations of claim 2.

7. As per claim 3, VeriSign covers a method as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). In addition, the supplementary certificate comprises the following data elements: signature algorithm, a key (the auxiliary attribute disclosed by Silberschatz modeled on the assignment of several keys to a user within a single certificate disclosed by Sutter), validity period of the certificate, extensions, and an identifying characteristic of the basic certificate. See VeriSign as modified by Stallings pg. 342, fig. 11.3(a) and pgs. 347-349, 'X.509 v3'; Sutter, 49:35-39; and Silberschatz, pgs. 7-8, sec. 1.3.1.1 and pgs. 52-58, figs. 2.20, 2.21, 2.22 and sec. 2.9.3.2.

8. Furthermore, VeriSign requires all CAs under the VeriSign PKI to retain records for all material events, including key generation, for the purpose of establishing an audit trail. See VeriSign, sec. 3.8 and 3.9. The inclusion of a key serial number in a certificate uniquely links the key to the key's history. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the supplementary certificate to store a key serial number. Motivation to combine include, inter alia, promoting users' trust in the certificate methodology. The aforementioned cover the limitations of claim 3.

9. As per claim 4, VeriSign covers a method as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). In addition, Sutter teaches certifying simultaneously

several keys in one certificate and Stallings teaches signing certificates by the trusted CAs. See VeriSign as modified by Sutter and Stallings, Ibid. The aforementioned cover the limitations of claim 4.

10. As per claim 5, VeriSign covers a method as outlined above in the claim 4 rejection under 35 U.S.C. 103(a). In addition, the certificate contains the following data elements: name of certification body, user id of certification body, name of user, user id of user, type and version of the certificate, key, validity, serial number, and extensions. See Stallings, pg. 342, fig. 11.3. Furthermore, inherent in the invention covered in the obviousness rejection of claim 4 is the inclusion of number and types of keys as data fields within the certificate. The aforementioned cover the limitations of claim 5.

11. As per claim 6, VeriSign covers a method as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). In addition, the creation of a new supplementary certificate to associate a new key pair with a basic certificate is analogous to creating a new supplementary entity to associate a new auxiliary attribute with a basic entity in an E-R model wherein a user is assigned to more than one certified key. The aforementioned cover the limitations of claim 6.

12. As per claim 7, VeriSign covers a method as outlined above in the claim 3 and 6 rejections under 35 U.S.C. 103(a). In addition, each supplementary certificate contain the following data elements: signature algorithm, key, serial number of key, validity

period of the certificate, extensions, and identifying characteristic of the basic certificate. See VeriSign as modified by Stallings pg. 342, fig. 11.3(a) and pgs. 347-349, 'X.509 v3'; Sutter, 49:35-39; and Silberschatz, pgs. 7-8, sec. 1.3.1.1 and pgs. 52-58, figs. 2.20, 2.21, 2.22 and sec. 2.9.3.2. The aforementioned cover the limitations of claim 7.

13. As per claims 8-11, they are method claims corresponding to claims 1-7 and they do not teach or define above the information claimed in claims 1-7. Therefore, claims 8-11 are rejected under VeriSign in view of Sutter, Stallings, Karlton and Silberschatz for the same reasons set forth in the rejections of claims 1-7.

14. As per claim 12, VeriSign covers a method as outlined above in the claim 8 rejection under 35 U.S.C. 103(a). In addition, the key is a public key. See Stallings, pg. 342, fig. 11.3(a), subject's public-key info. The aforementioned cover the limitations of claim 12.

15. Claims 13-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over VeriSign in view of Sutter, Stallings, Karlton and Silberschatz, and further in view of Deo et al. U.S. Patent No. 5,721,781 (hereinafter Deo).

16. As per claims 13 and 14, VeriSign covers a method as outlined above in the claim 4 rejection under 35 U.S.C. 103(a). VeriSign does not expressly teach storing the generated certificates in the non-volatile memory of a chipcard. Deo discloses an

authentication system wherein certificates are stored in non-volatile memory of a smart card. See Deo, 12:7-22; fig. 2, ref nos. 24 and 26. It would be obvious to one of ordinary skill in the art at the time the invention was made to store the generated certificates in the non-volatile memory of a smart card. Motivation to combine include, inter alia, enabling the user to mate the benefits of smart card secure static storage capability with certificate key authentication methodology. See Deo, 1:55-67. The aforementioned cover the limitations of claims 13 and 14.

17. Claims 15 and 17-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over VeriSign in view of Sutter, Stallings, Karlton and Silberschatz, and further in view of JAVA 'X.509 Certificates and Certificate Revocation Lists' (hereinafter JavaAPI).

18. As per claim 15, VeriSign covers a method as outlined above in the claim 14 rejection under 35 U.S.C. 103(a). In addition, Deo discloses the certificate is stored/loaded into the RAM of a smart card. See Deo, 12:7-22; fig. 2. Further, static sensitive data stored on a smart card are conventionally stored in the non-volatile portion of a smart card, since smart cards typically are only powered when attached to a smart card reader (see Deo, fig. 2, ref no. 28); and for the purpose of transferring the sensitive data or manipulating the sensitive data, the sensitive data is conventionally read into RAM. Examiner takes Official Notice of this teaching. It would be obvious to one of ordinary skill in the art at the time the invention was made to check the nonvolatile storage medium for the presence of certificates and read-in certificates from

the non-volatile memory into RAM to manipulate the certificate within the smart card as known to one of ordinary skill in the art.

19. Finally, VeriSign does not teach checking for the presence of a group certificate when no basic certificate is identified. JavaAPI teaches a software API implementing an abstract class named "certificate" for managing a variety of certificates having different formats but common uses. See JavaAPI, pg. 4, "What Java API can be used to access and manage Certificates". In the case when more then one certificate type exists for a common use, it would be obvious to one of ordinary skill in the art at the time the invention was made to check for the presence of a group certificate when no basic certificate is identified since a variety of certificates having different formats can be use to certify a key as known to one of ordinary skill in the art and as taught by JavaAPI. Ibid. The aforementioned cover the limitations of claims 15.

20. As per claims 17 and 18, they are method claims corresponding to claims 14 and 15 and they do not teach or define above the information claimed in claims 14 and 15. Therefore, claims 17 and 18 are rejected under VeriSign in view of Sutter, Stallings, Karlton, Silberschatz, Deo and JavaAPI for the same reasons set forth in the rejections of claims 14 and 15.

21. As per claims 19-25, VeriSign covers a method as outlined above in the claim 1-7 rejections under 35 U.S.C. 103(a). Furthermore, VeriSign discloses the step of a

specification of a request for certification of one of several keys by a certification body for a user. See VeriSign, sec. 4, 'Certification Application Procedures', esp. sec. 4.2.

22. VeriSign does not expressly disclose the method incorporated into a computer program product on a computer usable medium. JavaAPI discloses a certificate API software code utility to access and manage certificates. See JavaAPI, pg. 4, java.security.cert package. It would be obvious to one of ordinary skill in the art at the time the invention was made to implement the methods disclosed by VeriSign into a computer program product using the certificate API. Motivation to combine include, inter alia, enabling the method covered by VeriSign to be implemented into a marketable product as known to one of ordinary skill in the art and as disclosed by JavaAPI. Ibid. The aforementioned cover the limitations of claims 19-25.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W Kim whose telephone number is (571) 272-3804. The examiner can normally be reached on M-F 9:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jung W Kim
Examiner
Art Unit 2132

Jk
November 30, 2004

THOMAS R. PEESO
PRIMARY EXAMINER